

*Special thanks to
Marc Romanych and
Rachel Kitson for their
countless hours of editing
and comments that
significantly shaped the
resulting work.*

Lieutenant Colonel Norman E. Emery, U.S. Army, is an information operations officer assigned to 1st Information Operations Command (Land), Fort Belvoir, VA. A veteran of several Afghanistan and Iraq tours, he has performed Army and Joint IO duties since 1997 for the 101st Airborne Division (Air Assault), Multi-National Forces-Iraq, and in support of various special operations organizations. He holds an M.S. from the Naval Postgraduate School and has had six articles on IO/terrorism/insurgency previously published in the IO Sphere, Military Review, and the Journal of Information Warfare. LTC Emery welcomes comments, questions, and thoughts at norman.emery@us.army.mil, or norm.emery@gmail.com.

PHOTO: Iraqis crowd around U.S. Army Soldiers in a market in the Rashid District of Baghdad, Iraq, 24 September 2007. The Soldiers distributed Iraqi memorabilia and gathered information about the area. (U.S. Navy, Petty Officer 3d Class David Quillen)

Irregular Warfare Information Operations: Understanding the Role of People, Capabilities, and Effects

Lieutenant Colonel Norman E. Emery, U.S. Army

In this type of war . . . the task is to destroy the effectiveness of the insurgents' efforts and his ability to use the population for his own ends.

—Air Force General Curtis E. Lemay¹

OPERATION IRAQI FREEDOM (OIF) and Operation Enduring Freedom (OEF) do not qualify as conventional or unconventional warfare, but lie somewhere in between the two. Conventional U.S. military units in Iraq and Afghanistan find themselves engaged in operations best described as “special” rather than conventional or irregular. Labeled as irregular warfare, these conflicts actually have little resemblance to familiar doctrinal concepts. Once in theater, forces are required to engage using unfamiliar skills in political, economic, and social networking to complement military operations. We should not overlook the complexity of the enemy we face: a nexus of terrorism, insurgency, criminality, and negative transnational factors—a collective threat that does not always adhere to conventional ethics and rules.² Nor should we overlook the critical fact that all actors, state and non-state, are competing for the same objective: the people.

This set of circumstances requires information operations (IO) markedly different from those used in traditional conventional warfare. In irregular warfare, non-lethal capabilities have a more prominent and necessary role than in conventional warfare. Information operations directly influence the irregular warfare operational focus—the relevant populations. Current joint and Army IO doctrines do not adequately address the challenges long-term stability operations confront—irregular adversaries and asymmetric conflict. The doctrine still emphasizes the adversary decision-maker while minimizing the importance of the projection of public information to key non-adversarial audiences, especially foreign populations within the area of operations. These are critical tasks requiring greater expertise and an understanding of the irregular warfare information environment. To succeed in irregular warfare, IO officers need to understand how irregular warfare compares to conventional and counterinsurgency (COIN) warfare, the importance the population plays, how various adversaries project their information, and the importance for proficiency in cultural studies and studies of human behavior. Information operations planning must consider actions to support the tactical operation and the hierarchy of effects in the information environment that affect a unit's area of operations and influence.

We must reexamine IO officers' roles and education, proposed operations, and current IO doctrine, so that we do not continue to prepare Soldiers to fight today's war with yesterday's IO tactics, techniques, and procedures. An

Report Documentation Page				Form Approved OMB No. 0704-0188	
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.					
1. REPORT DATE NOV 2008		2. REPORT TYPE		3. DATES COVERED 00-00-2008 to 00-00-2008	
4. TITLE AND SUBTITLE Irregular Warfare Information Operations: Understanding the Role of People, Capabilities, and Effects				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Army Combined Arms Center, Military Review, Truesdell Hall, 290 Stimson Ave., Unit 2, Fort Leavenworth, KS, 66027				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution unlimited					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT Same as Report (SAR)	18. NUMBER OF PAGES 12	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified			

examination of irregular warfare IO must not just impart vignettes, lessons learned, and professional opinions: it must consider how IO challenges in current combat zones necessitate adjustments and adaptations. The current complex war environment indisputably requires this change.

Irregular Warfare and Relevant Populations

The U.S. Department of Defense (DOD) has developed an irregular warfare joint operating concept to define and develop key elements and strategy for current and future conflicts that reside on the spectrum between conventional and unconventional warfare. The joint operating concept defines irregular warfare as “a violent struggle among state and non-state actors for legitimacy and influence over the relevant population.”³ Irregular warfare is a form of armed conflict, as well as a form of warfare encompassing insurgency, counterinsurgency, terrorism, and counter-terrorism. COIN, a spectrum of actions taken by a government to defeat insurgencies, is a component of irregular warfare, and therefore most COIN principles and models apply to irregular warfare, which is a different, but not a lesser form of conflict than conventional warfare.⁴ While conventional warfare is direct military confrontation between states, irregular warfare focuses on the control and influence of populations, rather than the control of an adversary’s forces or territory.⁵ With irregular warfare, the problem is one of balancing operations against the enemy with operations to influence the population.

In conducting irregular warfare, one can neither ignore the enemy nor the population, and addressing them with equal energy and focus is difficult. The challenge in irregular warfare is that the adversary is not a single, easily characterized entity. In Iraq and Afghanistan, the insurgencies are not united monoliths; the “enemy” includes nationalists, protectionists, extremists, rejectionists, criminals, and terrorists—or any combination thereof. Separating the populace from the insurgents is a basic objective of COIN strategy. However, separating the terrorists

from the insurgents in irregular warfare is another matter entirely.⁶

For simplicity’s sake, the term anti-government forces here refers to all groups, regardless of motivation, collectively engaged in armed conflict against either coalition forces or a state’s legitimate security forces or both. No single term can properly categorize disaggregated groups that share common goals but have competing objectives. This lack of congruity among objectives makes the collective groups vulnerable to effective IO that can drive a wedge between tenuous relationships and convenient partners.

The human terrain. Neither our enemies in irregular warfare nor the relevant population are monolithic. Lieutenant General Peter Chiarelli demonstrated an understanding of this fact when he commanded the 1st Cavalry Division in Baghdad in 2004. He emphasized the need for coordinating combat, stability, and information operations to create a stable and secure environment in Sadr City. Key to ensuring focused efforts was an understanding of anti-government forces’ competition for the population and approaching the population as three distinct constituencies—opposed, unopposed, and undecided (figure 1).⁷ Understanding these groups can help us better determine appropriate operations (e.g., lethal or non-lethal) and the messages to deliver.

Opposed audiences are active anti-government forces members or actively support the various enemy groups, and therefore are opposed to the state or ruling authority. The unopposed simply support the government. While the two sides struggle to dislodge each other, the true battleground is the constituency of the undecided, the “fence-sitters.”⁸ The undecided are generally waiting out progress and security concerns to determine who they will support; the victor will be the one who gets them off the fence. It becomes a zero-sum game for the state, the military, and the anti-government forces as they each compete for the bulk of the population that has yet to commit and can be swayed with the promise of hope or the threat of violence.⁹

The U.S. military should accept that instead of winning over these people, “victory” may consist

In conducting irregular warfare, one can neither ignore the enemy nor the population, and addressing them with equal energy and focus is difficult.

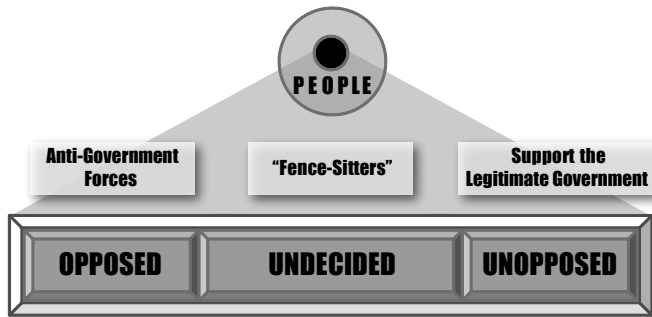


Figure 1. The three population constituencies in irregular warfare.

of simply not losing them to the enemy. A mantra the U.S. military often uses to describe its efforts to maintain the unopposed and sway the “fence-sitters” is “winning the hearts and minds.” Too often a hearts-and-minds campaign is interpreted as making the population “like” us, but it really means reaching a population through emotive and cognitive means.¹⁰ It is more than noble efforts in building infrastructure, holding elections, and creating jobs. Occupiers have to leverage existing social and political networks and build support within these networks to separate the insurgency from the population.¹¹

Irregular warfare conflict model. Several conflict theory models have addressed the population’s role in warfare, the most well-known being Prussian strategist Carl von Clausewitz’s, which addresses warfare’s trinity: military, government, and people. According to Clausewitz, military operations focus on an opposing state’s armed forces as a means to control the government in the belief that the population will follow the lead of the government and accept the political outcome. An example would be Japan’s surrender in World War II. The only military objective involving the population was minimizing civilian interference with operations. The trinitarian conflict model, a variation of Clausewitz’s trinity and a principle of COIN theory, portrays non-state actors pursuing the Clausewitz paradigm in reverse order by confronting the people first to influence the government and avoid directly confronting the military.¹² The

non-state actor has a greater chance of defeating the government if it gains the majority support of the population; if the government falls or compromises, that negates the non-state actor’s need to attempt to decisively engage the military.¹³

Figure 2 depicts the Clausewitzian trinity adapted for irregular warfare and portrays the critical and common element to both the state’s and insurgents’ success: the people. This model, a variation of one developed by a retired Special Forces officer with significant COIN experience, portrays how the population is coveted by the state and its military to remain supportive of the legitimate government.¹⁴ The mirrored model illustrates the military’s and insurgents’ preferred approach to engaging and winning the population rather than pursuing exclusive armed engagements. In a basic COIN model, the U.S. provides limited assistance, such as the current support in the Philippines.

The irregular warfare model in figure 2 depicts direct U.S. involvement with a cooperative state, the population, and the insurgents and represents current operations in Iraq and Afghanistan. Essentially, because irregular warfare is a social-political crisis, this type of warfare requires more than a pure military solution.¹⁵ The political and psychological aspects of irregular warfare are just as important as the physical actions. With the people the center of focus, information operations play a very significant role.

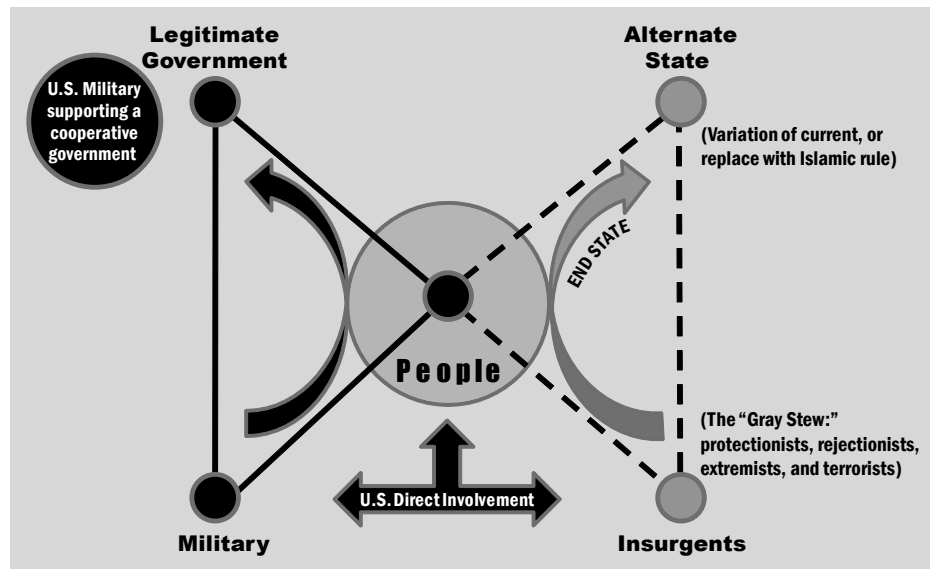


Figure 2. Clausewitz’s “trinity” (military, government, people) adapted for irregular warfare with U.S. military direct involvement.

IO Challenges in Irregular Warfare

“Irregular warfare is about people, not platforms.”¹⁶

The key military objective in irregular warfare—the relevant population—is also important for IO because this is our target audience. How an audience directly and indirectly reacts to messages affects how and when the United States achieves its campaign objectives. It is important to understand our primary audience, and remember how easy it is to lose focus by pursuing tomorrow’s or reacting to yesterday’s headlines, instead of sticking to a uniform message in support of a long-term strategy.

We should seek to shape the information environment for long-term success, and not bog ourselves down in point/counterpoint with adversaries striving for notoriety. Public affairs can counter specific adversary actions, but IO collectively should counter adversary strategies.¹⁷ To achieve their goals, commanders and IO officers have to understand the information environment. The information environment is part of the operating environment and grounded in the physical domain. It consists of three dimensions: physical, informational, and cognitive.¹⁸ All communication systems, including human information networks, reside in the physical dimension. The informational dimension “consists of the content and flow of information.”¹⁹ The cognitive dimension is the most important; in this realm, the decision-makers and target audiences think, perceive, visualize, and decide.²⁰ Simply put, if you were at a computer terminal, the computer is the physical dimension, the informational dimension is the data flowing through the computer, and viewing and processing that data is the cognitive dimension.

Know your audience. A shortcoming of IO doctrine is that its primary focus is on influencing critical adversarial decision-makers. This approach neglects a key target of irregular warfare: the relevant population not categorized as adversarial. The DOD IO Roadmap, produced 7 months after the invasion of Iraq and 25 months after entering Afghanistan, asserts that IO “must be refocused on adversary decision-making.”²¹ It fails to acknowledge a necessity, let alone a role for IO, in building relationships with civilian populations. It fails to grasp that effectively communicating the U.S. military’s message to local, regional, and international

A shortcoming of IO doctrine is that it...neglects a key target of irregular warfare: the relevant population not categorized as adversarial.

populations is a means of helping to achieve tactical and operational military objectives.²²

By failing to understand the various audiences, we pursue or react to information or incidents with actions that seek to blanket all the audiences, making it costly and not fully effective. A common mistake in irregular warfare is to develop and disseminate a one-solution/message-for-all approach. It is inefficient to expend resources trying to convince an audience already committed to us. We should therefore avoid blanket messaging and instead, using minimal resources, make “maintenance” or reinforcement efforts toward the unopposed audiences, and put full effort toward the undecided audience. This is a strategy U.S. politicians employ during national elections. Thus, within one theme/message/information goal, there could be variations targeting adversary decision-makers as well as the three constituencies and their key non-adversarial leaders, such as tribal leaders, imams, and civic and political leaders.

In irregular warfare, not every possible audience or adversary can be persuaded to reconcile, and therefore, combat operations are required to destroy these groups. Information operations planning must consider not only actions to support the tactical operation, but also the hierarchy of effects in the information environment that affects a unit’s operational area. A commander engaging physical, informational, and cognitive dimensions at the tactical level can gain exposure at national, regional, and international levels, and the impact in the cognitive dimension can have positive or negative effects on future operations for all commanders in theater. Joint doctrine dictates that at key points in time and space during conflict, the U.S. military should achieve and maintain information superiority, i.e., “the operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary’s ability to do the same.”²³ In irregular warfare,

the military, despite its technology, will rarely, if ever, gain information supremacy, while achieving information superiority may be temporary with unpredictable fluctuations. We cannot prevent an adversary from putting out a message or information. What we can and should do is to set conditions in the information environment with the key audiences (unopposed, opposed, undecided), so when opposing messages come out, they do not resonate.

Our adversaries' information goal is to be first. A rumor-centric society rewards this achievement. However, being the first with a message is not necessarily a victory, and being second is not necessarily a loss. Our goal should be to be first with the truth. Sometimes the enemy gets out the first word, but we can render it irrelevant by staying on message and by consistently repeating mutually supporting themes. In the end, our adversary has not necessarily gained success by delivering his message, nor has he dealt a defeat to us, just as our delivery of a message is not in itself a success. The issue is how the message resonates with target audiences. A global information environment in which most people believe the first story out tempts us to respond with a strategy of short engagement actions instead of adhering to enduring actions. Insurgencies have historically lasted 9 to 12 years, so one should not view irregular warfare IO efforts as short-term.

There are no well-codified rules in irregular warfare, but in competing for the population, terrorist and insurgency groups must at least abide by the rule of understanding their audience. The descent into barbarity (beheadings, deadly bombings) by such groups as Al-Qaeda in Iraq does not persuade the fence-sitters, and may cause the terrorists to lose the support of their constituents. Adversaries competing within a state (such as in Iraq, home to numerous

Sunni insurgents, moderate and extremist) can lose audiences by bombarding the populace with conflicting messages. This is to the coalition's advantage. It is critical to develop and reinforce themes and messages that are consistent over time and coordinated with Iraqi and Afghan governments.

Good news stories and U.S. popular support.

Since information is central to the ability to shape battlefields, unity of effort and purpose in the information environment is vital.²⁴ While there must also be unity of information for indigenous and global audiences, if we concentrate on winning the local audience first, U.S. and global audiences will follow.²⁵ Information operations and public affairs officers at the operational level face a dilemma when they encounter military leaders who believe there is a need to push "good news" stories to counter the perception that only tragedy, hardship, and failure occur in combat zones. This tactic clearly aims at U.S. audiences, as Iraqis want proof and perception of physical security, not stories of school openings. Unfortunately, the "good news story" became a misguided sprint strategy, as some military leaders perhaps believed they had a responsibility to balance, if not counter, the output of U.S. news channels and newspapers to maintain U.S. domestic support. Any serving member knows of positive successes, but relating such stories can be a challenge, even with supportive media. In a 2006 article, journalist Lara Logan wrote of her frustration in getting relevant data from a general officer who wanted to share a "good news story" with her.²⁶ She tried to get the "good news" facts, but the officer could only assert such things as security was "better," great "progress" was being made. They had removed 100,000 cubic feet of trash from neighborhoods and operations were moving toward the goal of improving electricity for 3,000 homes.²⁷ Any leader who attempts to portray *national level* progress with the results of *tactical projects* would understandably receive a tepid response. Progress is the sum of achievements and atmospherics and is difficult to articulate; nevertheless, those operating in the combat environment can "sense" it, and it is a nuance of the information environment.

Our leaders must recognize that a single achievement can seem insignificant when taken out of the context of overall progress or buried amid the reporting of turmoil. As the military relies more

The descent into barbarity (beheadings, deadly bombings) by such groups as Al-Qaeda in Iraq do not persuade the fence-sitters, and may cause the terrorists to lose the support of their constituents.

on commanders to convey progress, public affairs officers (PAOs) are doing far fewer visual and print interviews than might be expected. This shift in communication requires that leaders understand the trap of relaying empirical tactical progress to U.S. audiences who do not view the conflict in terms of city sectors. These leaders must better articulate progress so that it does not sound hollow. One method is to relate success that has or will occur over time using objective and empirical metrics. An example: "A new power plant opening in town X will provide reliable electricity to several hundred homes and create 70 new jobs in a region where men have resorted to insurgent activity to provide for their families. This will likely result in a vastly improved security situation in the coming months, and is a model of progress that is proving successful in this region."

The enemy has no rules. The non-state actor reigns supreme in the information environment. Information is the commodity with which it purchases cooperation, survivability, the perception of victory, and silence amongst supporters. The terrorist and insurgent do not have an IO doctrine. According to Jim McNieve, 1st IO Command (Land), non-state actors commonly use three broad methods in their information effects strategy:

- Projection of their message to various target audiences.
- Protection of vital information to enhance survivability and decision-making.
- Collection of information on their enemies.²⁸

Our adversaries understand how to leverage the information environment, and the U.S. military should not abdicate that battlespace in pursuit of perpetual raids and kill-or-capture operations. Because the anti-government forces do not have military parity with the U.S., they do not seek success on the streets but in the information environment. They are not bound by the rules and ethics of responsibly releasing truthful information. The enemy has no rules. It can exaggerate claims, sensationalize events, omit facts, purposely mislead, and release information quickly without extensive staffing. In past decades, the way to reach audiences was the traditional media,²⁹ but now it is the Internet, where "the keyboard equals the Kalashnikov."³⁰ In irregular warfare, the gap between U.S. and adversary IO capabilities and use of the media and the Internet is much smaller than the gap between

Our adversaries understand how to leverage the information environment, and the U.S. military should not abdicate that battlespace in pursuit of perpetual raids and kill-or-capture operations.

their respective military force capabilities. Islamic terrorist and insurgent groups we once considered ignorant and primitive are making effective use of cyberspace as a communication medium. This includes not just command and control via the Internet, which we expect in the 21st century, but the proliferation of messaging and propaganda directly connected to anti-government forces engagements in Iraq and Afghanistan, especially those causing or exploiting U.S. and allied casualties. Groups increasing video output include Iraq's predominately Sunni Arab insurgency, as well as the Taliban, who ironically opposed the use of cameras when they ruled Afghanistan.³¹

Inevitably, other extremist groups will adopt this practice before long. Libyan firebrand Abu Laith al-Libi recently urged Islamic insurgents in Somalia, who have mostly ignored the medium, to begin using videos to foster awareness of their fight."³² Information operations not only project messages, but also seek to deny and degrade the adversary's messages and deny his access to and effectiveness on the Internet. Countering these videos is of urgent importance, because research shows that "Internet chat rooms and forums are replacing mosques as venues for recruitment and radicalization."³³ This course of action requires the U.S. military to engage adversarial operations and propaganda directly and indirectly on the Internet.

Leveraging Information Engagement Capabilities

Information operations are a key COIN logical line of operation to win the war of ideas and destroy the will and legitimacy of the insurgency, and IO have the same, if not greater, relevance in irregular warfare.³⁴ We should seek solutions to irregular warfare's IO challenges by closely coordinating of efforts among the array of capabilities that

engage the public. We should set aside the current IO doctrine of “core,” “related,” and “supporting” capabilities. Such artificial categories create false barriers to planning, coordinating, and executing IO in irregular warfare. The IO core capabilities listed in current doctrine—“psychological operations” (PSYOP), “electronic warfare” (EW), “computer network operations” (CNO), “operations security” (OPSEC), and “deception”—have a logical but unnatural grouping, and constrain leaders’ views of IO—by portraying it as *five* capabilities.

While an important guide, doctrine should be just a point of departure in the constantly evolving irregular warfare environment. Information operations is not a grouping of capabilities that comprise information. Information operations is a grouping of capabilities that affect information. More importantly, IO have a specific purpose and emphasis within an overall plan of action, operate under the same dynamics, and are inseparable from kinetic combat operations.³⁵ Information operations are more than just public affairs and PSYOP releases after a mission. Tactical commanders in Iraq and Afghanistan have had success with public information engagement as a main effort. Public information should consist of the coordinated, combined efforts of public affairs, PSYOP, civil affairs, combat camera, and face-to-face engagement. These capabilities are critical because irregular warfare requires a de-emphasis on information technology.

Holding your enemy close: making PA, PSYOP, and IO work. Unity of information effort is vital in irregular warfare. The two key specialties of PSYOP and public affairs (by doctrine, a “related” capability) support each other in today’s combat environments. Still, they differ in coordination and execution. Many who work in public affairs think of PSYOP, and by extension IO, as nonfactual or even subterfuge—as manipulative and potentially mendacious marketing campaigns. Leaders can dilute the value of IO by thinking of it merely as an equivalent of public affairs or PSYOP. However, it is not heresy to group public affairs and PSYOP into a coordinated public information construct. Both use similar means (relaying a truthful message to specific audiences) to achieve different objectives (public affairs informs and PSYOP influences). A coordinated effort maximizes message effectiveness.

Brigade or regimental combat teams must develop the capability to influence and inform key target audiences at the local level. One commander even reported that his brigade’s main targets were Iraqi and Arab media, “because they informed the population in my area.”³⁶ We should influence and inform key target audiences through the local media or face-to-face means, because a national release by a theater PAO is insufficient to reach the fence-sitters and the uncommitted. In many ways, we do not use public affairs enough in irregular warfare foreign media operations. We have to reach a unit’s tactical target audience population. Public affairs in support of irregular warfare should be more than just informing the U.S. public.

However, the joint definition of information operations, the integrated employment of capabilities “to influence, disrupt, corrupt, or usurp adversarial human and automated while protecting our own,” limits public affairs application in irregular warfare.³⁷ The definition does not address non-adversarial populations, and does not include “inform,” thereby blocking public affairs involvement, in coordination with IO, to reach specific foreign audiences. Commanders cannot succeed without public affairs and PSYOP capabilities to disseminate one-voice messages that engage tactical audiences, foreign media, and foreign populations, and coordinate counter-propaganda efforts. This issue is not one of public communication, but one of foreign communication.³⁸ public affairs (inform using unclassified messaging) and PSYOP (influence using classified messaging) converge with respect to foreign media operations; PSYOP can extend the message’s momentum as the public affairs-driven news cycle winds down.³⁹ Engaging foreign audiences with one capability without coordinating with the others increases the likelihood that PSYOP will encroach into public affairs’s lane. Ironically, for public affairs to protect its contribution to the mission, it *must* work closely with PSYOP and IO planners.

Public affairs and PSYOP should cooperate in influence operations because the military has too few trained communicators to deal adequately with the overwhelming information demands of irregular warfare.⁴⁰ The PAO is an invaluable information battlespace advisor to the commander. He or she naturally understands the information environment as a whole. If the PAO excuses

himself from a process in which he is encouraged to participate, the commander will have to make information decisions without public affairs advice, even though the PAO is the best-qualified officer to give such advice. If public affairs is committed to success of the command, it will be part of the staff IO planning.

By doctrine, combat camera and face-to-face engagement are not IO, but they fall within information engagement capabilities. They therefore reinforce IO as part of operations, not a grouping of capabilities that various staffs “own.” Face-to-face engagement is relevant and valuable at the tactical and operational level. It is a delivery platform to achieve information effects that inform, influence, or co-opt. Face-to-face engagement is a technique to engage influential leaders (municipal, national, civic, and tribal) before and after operations. Implementation by a commander instead of an IO officer does not mean it is not an IO function. Information operations strives to achieve specific results in the information and cognitive domains; the executing agents vary depending on which is the most appropriate. The combat camera capability supports IO by documenting events and operations to exploit successes, mitigate post-mission misperceptions, or counter accusations. We should view face-to-face engagement and combat camera as a valuable part of a strategy to integrate key public information elements and tools to achieve effects.

The final capability that plays a significant role in irregular warfare IO is civil-military operations, usually coordinated by civil affairs personnel.⁴¹ Civil affairs is an IO-related capability and has a valuable role in achieving tactical cognitive effects. Information operations does more than just synchronize PSYOP with civil-military operations. Civil-military operations can affect social and political change in communities and regions through infrastructure work and social services, which have an important affect on target populations. Although some say “civil-military operations is not IO,” they fail to recognize that civil-military operations is an important irregular warfare tool the commander can use to achieve informational and cognitive objectives in a target audience. While civil affairs can be altruistic, its function is to help the commander affect information environments and his operations. Purposeful philanthropy is for non-governmental organizations.

Public affairs, civil affairs, and PSYOP officers are effective in executing their respective functions in support of commander’s guidance regardless of an IO officer’s presence on staff. And the presence of an IO officer in centrally coordinated information operations does not necessarily subordinate those fields or erode their status with a commander. A public affairs officer can always say “no” to the recommendations of an IO officer. Centrally coordinated IO in irregular warfare does offer a method to eliminate seams between areas of expertise and capabilities. Ideally, the IO officer is in a position to have wide conceptual visibility. Such visibility enables an ability to coordinate and synchronize public affairs, civil affairs, PSYOP, face-to-face, and combat camera actions and information with respect to timing and effect within the area of operations.

The IO staff officer might suggest the timing or development of a PSYOP or public affairs product; recommend civil-military operations in support of non-lethal objectives to persuade non-military (tribal, religious, government) leaders; recommend combat camera document a certain operation; or suggest a face-to-face engagement before or after an operation. These suggestions or recommendations to the commander or chief of staff should diminish seams and achieve a greater effect. One of the IO officer’s greater contributions in irregular warfare can be to eliminate seams and maximize effectiveness.

Understanding Effects in IW

“An effect is the power to bring about a result, i.e., influence.”⁴²

Measures of effectiveness are difficult to design and judge in a COIN campaign because, by nature, insurgencies are politically volatile and asymmetric.⁴³ This intractability prevails in irregular warfare for a number of reasons. The population’s diversity and antagonisms, the presence of hidden enemies, the complexities of time and space, and the difficulty of observing and measuring the success of actions, or even knowing if they are successful, all contribute to eluding any meaningful gauge.

In irregular warfare, measuring effectiveness involves more than just simply observing imagined cause and effect relationships or having immediate or timely feedback. It requires subjective and abstract metrics. We often apply empirical data awkwardly to measure subjective effects, and the

resulting information can have little significance if we do not properly define success. We should remain cognizant of the difference between measuring effectiveness and measuring success, which may be quite different entities. Empirical data best measures the success of tasks over time or helps analyze trends.

The hierarchy of effects. Information operations officers must understand first-, second-, and third-order effects and apply this knowledge to tactical planning in irregular warfare. They can best advise the commander on assessing information environment risk to daily combat operations by addressing first-, second-, and third-order effects to identify potential collateral effects that result in positive or negative outcomes.⁴⁴ First-order effects are associated with the physical dimension of the information environment, while second- and third-order effects are associated with the information environment's information and cognitive dimensions. There are few clear lines of demarcation beyond third-order effects.⁴⁵ A first-order effect is a direct effect, a result of actions with no intervening effect or mechanism between the act and outcome. Such an effect can trigger additional outcomes, which are indirect (second- and third-order) effects.⁴⁶ Given the complex irregular warfare environment, the IO officer must not only take into account probable adversary reactions to friendly operations and events, but also their impact on the population and its actions and reactions in response to them. Some examples of IO that support or mitigate each level of effects follow.

First-order effect—An immediate physical action or reaction. The IO goal is to enable force protection or unit success in executing the mission, limit adversary response, perhaps using EW and tactical PSYOP supported by tactical deception and stringent OPSEC countermeasures.

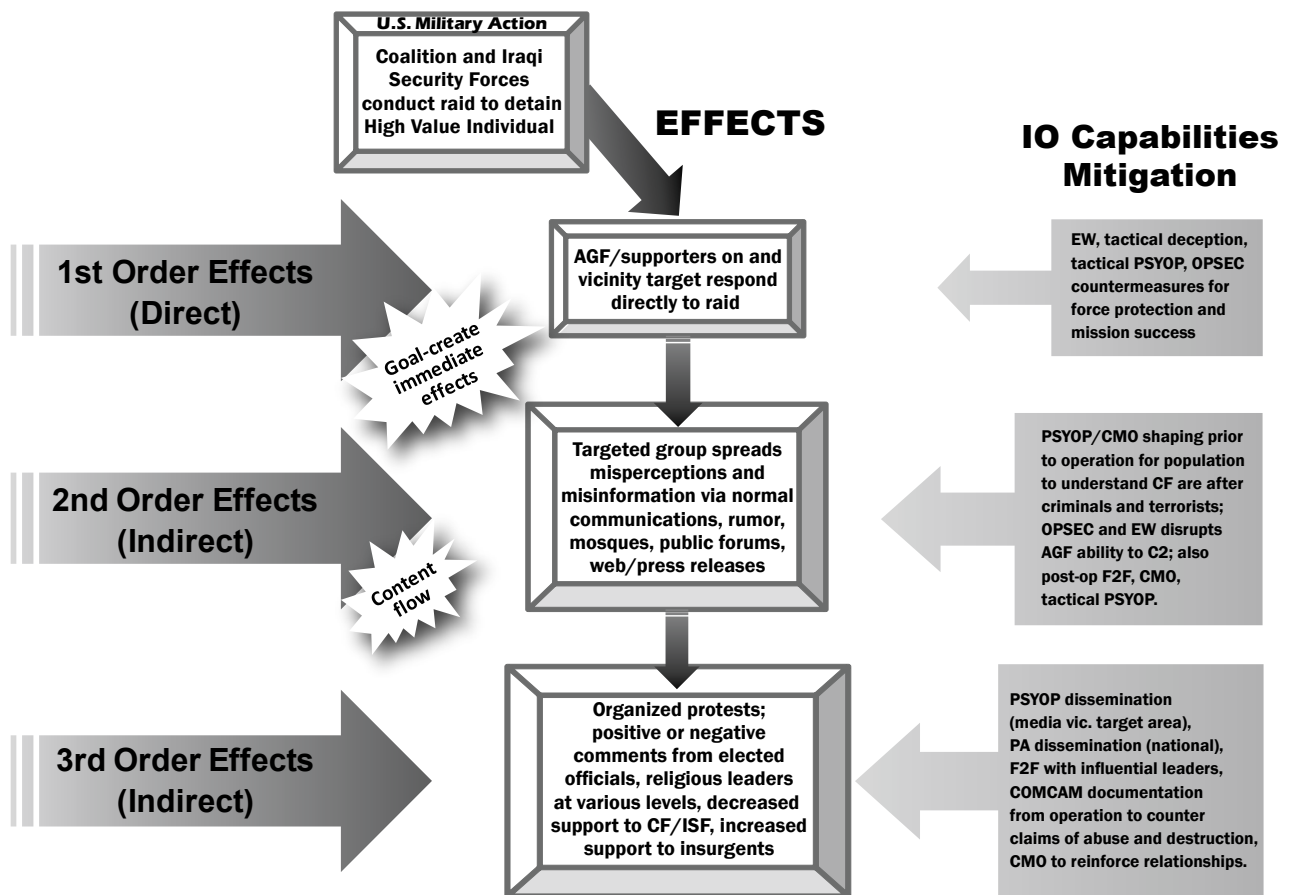
Second-order effect—The quality and integrity of information and information flow, EW, and tactical PSYOP actions limits disinformation resonating with the population. This could include an face-to-face meeting with an influential municipal or religious leader and coordinated civil-military operations to shape perceptions.

Third-order effect—Decision-making and perceptions. The IO officer coordinates various IO capabilities and other actions to support gaining

the desired effect or preempting, countering, or mitigating an effect, using public affairs, PSYOP, and face-to-face to disseminate information.

Figure 3 depicts how IO officers can assess an operation's risk and effects by applying certain actions. The figure illustrates a raid to capture an individual wanted for suspected terrorism or violent crimes. Understanding first-, second-, and third-order effects is necessary for planning to achieve desired IO objectives. An IO objective should be effects-based, describing a condition or state in the information environment that IO elements will attempt to achieve.⁴⁷ The irregular warfare challenge is that intelligence systems cannot always detect the disposition of a population or the response of insurgent forces to coalition efforts. Such responses are not quantifiable by empirical data anyway. Therein lies the flaw: trying to produce effects as though doing so were a science. Assessing the situation requires atmospherics and information that sometimes is not personally gathered or observed by U.S. forces, and not easily or best expressed with numeric data. The reasons can be the permissiveness of the environment and the availability, access, and cooperation of citizens for polling.

Applying an effects-based process. Determining desired hierarchy of effects and supporting actions to achieve information objectives is just as important as evaluating the hierarchy of effects for planned tactical operations. There is a difference in planning operations with effects and planning effects-based operations, and this difference is important in irregular warfare. "Effects are linked to desired objectives, exert influence, cause a result, or trigger additional outcomes."⁴⁸ The IO officer can use an effects-based relationship model to validate effect objectives and military operations that support them. The model helps the IO officer verify if he is truly gauging and calculating effects rather than performance. An effects-based planning approach will address "the mind perceptions and cognitive dimensions of an adversary's reality, regardless of any physical or military inferiority or superiority."⁴⁹ Effects-based planning is very much relevant in irregular warfare because it is centered on the conditions of that reality necessary to achieve success, which may not exclusively relate to an adversary.⁵⁰ This is essential when political and social factors are inseparable from military



LEGEND: AGF, anti-government forces; C2, command and control; CF, coalition forces; CMO, civil-military operations; COMCAM, combat camera; EW, electronic warfare; F2F, face-to-face; ISF, Iraqi Security Forces; OPSEC, operations security; PA, public affairs; PSYOP, psychological operations.

Figure 3. Evaluating hierarchy of effects for planned tactical operation.

operations to achieve campaign objectives. And it requires IO officers to think beyond the initial operation or IO action and prepare to address collateral or unintended effects.

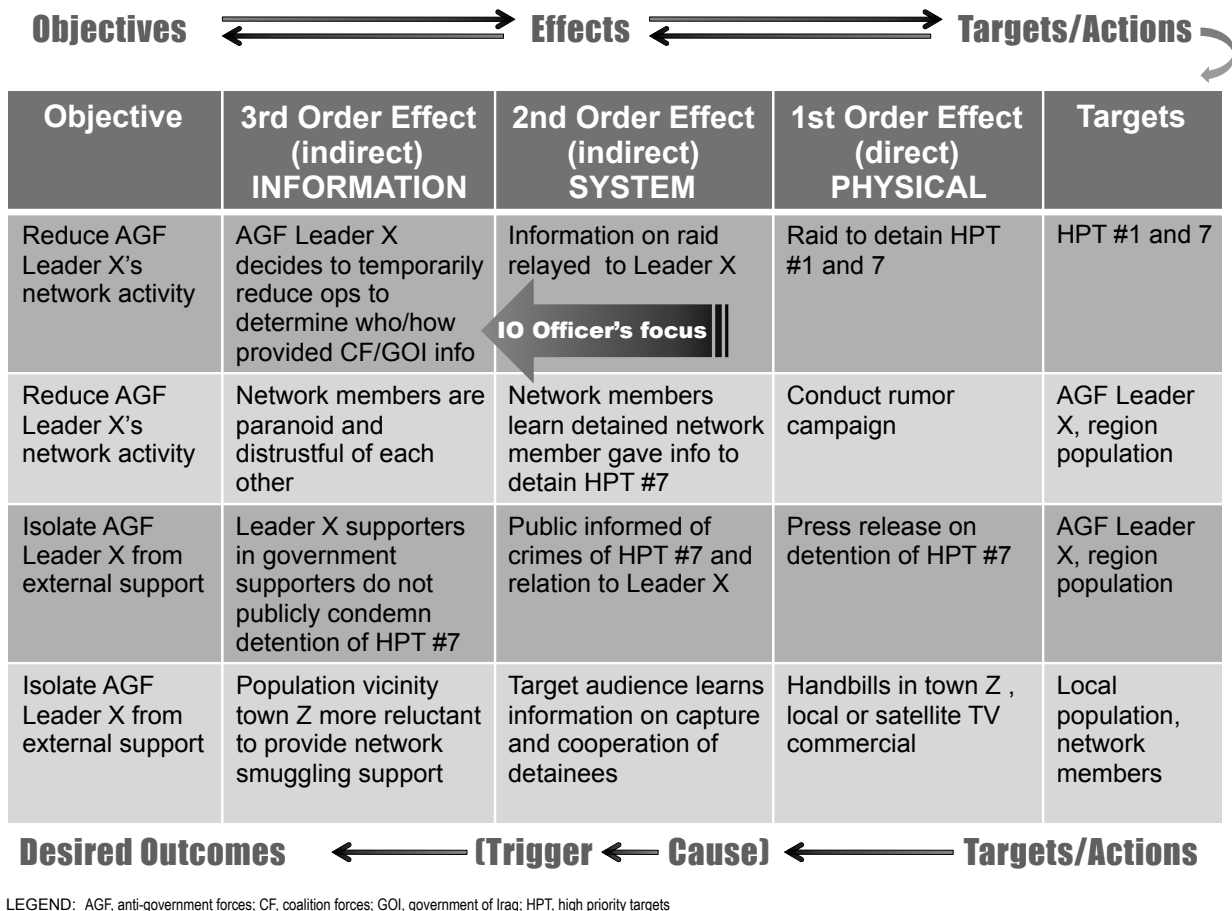
Figure 3 illustrated the hierarchy of effects applied to a tactical operation focused on the adversary. Figure 4 is an effects-based model adapted as an IO or effects planning tool; its original purpose was to show the relationship of objectives, effects, and targets.⁵¹ The intent is to easily identify required IO-related actions to support achieving irregular warfare objectives. The example uses a scenario of a commander's intent to reduce IED network activity in order to decrease lethal attacks against the population and U.S. Forces. The identified objectives are "reduce anti-government forces Leader X network activity" and "Isolate anti-government forces Leader X from external support." This results in planners identifying initial targets and actions, both lethal and non-lethal, and the resulting direct and

indirect effects. From the target, select likely first-, second-, then third-order effects, ending with the stated objective. This process is to ensure the target/action will likely produce the desired outcome. The IO officer evaluates if these likely effects (it is not possible to precisely predict or measure outcomes) are acceptable and makes necessary recommendations to the staff as needed. The IO officer is focused on getting the third-order effect to occur.

Information operations officers should have this breadth of understanding of operational risk and potential order of effects, although these are not exclusively IO functions to develop or gauge.

Conclusion

In the last seven years, prolonged U.S. engagements in Iraq and Afghanistan have had a major impact on military operations, as well as the role general forces play. The methods and processes proposed here are not definitive, but may expand



**Figure 4. Effect-based relationship model adapted for IO planning in irregular warfare.
(Relationship of objectives, effects, and targets)**

IO officer knowledge and thought processes for irregular warfare. My purpose is to share ideas and concepts with my peers, the IO proponent, and others responsible for training, educating, and preparing IO officers for OIF and OEF. Despite my ten years of Army and joint IO experience at tactical, operational, and theater levels, I continue to experience hard and sharp learning curves with each successive deployment.

An examination of warfare and IO doctrine is not only required of senior leaders, but also of those responsible for executing and coordinating operations in irregular warfare, and in the military education and training system responsible for preparing those individuals and forces.⁵² In irregular warfare, the role of IO is significantly greater than during major combat operations. The people among the populations and the roles they play in society, government, the military, and the insurgency are the foremost focus of IO methods in support of irregular warfare.

If all one has is a hammer, then the entire world begins to look like nails.⁵³ This observation also applies to what commanders and staffs believe IO represents. However, IO are more than just public affairs and PSYOP releases after a mission. Although the population's role in irregular warfare requires emphasis on IO public engagement, an enemy we once underestimated is demonstrating a more effective use of cyberspace as an internal and external communication tool, and this requires special "technical" IO attention and efforts. Moreover, at the tactical and theater levels in Afghanistan and Iraq, it is time for public affairs and PSYOP officers to define how they will cooperate and coordinate in support of the commander's information objectives, rather than continue to itemize the reasons they stay at arm's length. Continued friction only serves the adversary. We cannot prevent our adversaries from disseminating their messages, but we can affect how that message resonates with our target audiences.

Words alone will not have a tipping-point effect. Information operations is not a golden arrow or a silver bullet to counter and destroy enemy propaganda and quickly cause whole populations to change disposition. Doing so requires coordinated military operations. Information operations officers should be able to advise their commanders of the risks and potential direct, indirect, and collateral effects that physical domain operations will have on the information environment. In measuring the effects of operations, let us not make the process to evaluate them too hard.

Although force levels may decrease during the next few years, our commitment to victory will not. Our forces in Iraq and Afghanistan must understand and prepare for changing threat environments and their impact on the irregular warfare environment as our adversaries adapt and other opportunists surface when rivals are defeated. A rule to heed: do not underestimate these challenges just because you understood the information and threat environment during your last deployment.

MR

NOTES

1. Air Force Doctrine Document 2-3, *Irregular Warfare*, 1 August 2007, vi.
2. Joseph D. Celeski, *Operationalizing COIN*, JSOU Report 05-2. (Hurlburt Field, FL: The JSOU Press, September 2005), 82.
3. *Irregular Warfare Joint Operating Concept*, 4, Department of Defense.
4. AFDD 2-3, 8.
5. *Irregular Warfare Joint Operating Concept*, 6.
6. Celeski, 82.
7. Peter W. Chiarelli and Patrick Michaelis, "The Requirement for Full Spectrum Operations," *Military Review* (July-August 2005): 8.
8. Ibid.
9. Celeski, 82.
10. David J. Killcullen, "Counterinsurgency in Iraq: Theory and Practice: 2007," Conference, PowerPoint presentation.
11. Nick Dowling, "COIN flip," Opinion Back Talk, *Army Times*, 9 July 2007, 46.
12. Norman E. Emery, "Information Operations in Iraq," *Military Review* (May-June 2004): 11.
13. Ibid.
14. U.S. Army Colonel (retired) Joseph Celeski commanded Combined and Joint Special Operations Task Force-Afghanistan in 2002 and authored *Operationalizing COIN*.
15. Celeski, 38.
16. *Irregular Warfare Joint Operating Concept*, 1.
17. Ibid., 2.
18. JP 3-13, *Information Operations*, 13 February 2006, I-1.
19. Ibid., I-2.
20. Ibid.
21. Department of Defense, "Information Operations Roadmap," (October 2003), 22.
22. Andrew Y. Badger, "Information Operations in Counterinsurgency: The U.S. Experience in Iraq" (Thesis, Harvard University, 2007), 15.
23. Joint Publication (JP) 3-13, GL-9.
24. Curtis D. Boyd, "Army IO is PSYOP: Influencing More with Less Military," *Military Review* (May-June 2007): 72.
25. Killcullen.
26. Lara Logan, "Too Late for Baghdad?" CBS News.com, September 18, 2006, <www.cbsnews.com/stories/2006/09/18>.
27. Ibid.
28. James McNeive, unpublished concept, 1st Information Operations Command (Land), 2006.
29. Fred Lucas, "Internet a Front Line in Terror War, Reports Warn," *Cyber News Service*, 27 June 2007. Compiled by Jeff Harley in *Information Operations Newsletter*, 7, no 17, U.S. Army Strategic Command (1 June-17 July 2007).
30. Substituting the computer and the AK-47 in a reworking of "the pen is mightier than sword."
31. Jim Krane, "Experts: Al-Qaida Boosts Video Offensive," Associated Press, 1 June 2007. Compiled by Jeff Harley in *Information Operations Newsletter*, 7, no 17, U.S. Army Strategic Command (1 June-17 July 2007).
32. Ben Venzke quoted in Krane.
33. Lucas.
34. Celeski, 53.
35. William Darley, "Clausewitz's Theory of War and Information Operations," *JFQ*, (1st QTR 2006): 73, 79.
36. Ralph O. Baker, "The Decisive Weapon: A Brigade Combat Team Commander's Perspective on Information Operations," *Military Review* (May-June 2006): 26.
37. JP 3-13, ix.
38. Boyd, 72.
39. Ibid., 74.
40. Tadd Sholtis, "Public Affairs and Information Operations: A Strategy for Success," *Air and Space Power Journal* 19, no.3 (Fall 2005): 102.
41. Civil affairs (CA) is the career field; CA soldiers conduct civil military operations.
42. Edward C. Mann III, Gary Endersby, and Thomas R. Searle, *Thinking Effects: Effects-based Methodology for Joint Operations*, CADRE Paper No.15 (Maxwell Air Force Base, AL: Air University Press, October 2002), 30.
43. Celeski, 59.
44. Mann, 35.
45. Ibid., 34.
46. Ibid., 31.
47. David C. Grohoski, Steven M. Seybert, and Marc Romanych, "Information Operations with a Purpose," *IO Sphere* (Spring, 2005): 32.
48. Mann, 40.
49. David B. Lazarus, "Effects-Based Operations and Counterterrorism," *Air & Space Power Journal* 19, no.3 (Fall 2005): 24.
50. Mann, 43.
51. Ibid., 35; original model demonstrating air operations and effects are replaced with IO actions in support of IW operations.
52. Ahmed S. Hashim, *Insurgency and Counter Insurgency in Iraq* (Ithaca, NY: Cornell University Press, 2006), 328.
53. Unattributed axiom quoted in Roger W. Barnett, *Asymmetric Warfare: Today's Challenge to U.S. Military Power* (Dulles, VA: Brassey's Inc, 2003), 88.